AMENDMENTS TO THE DRAWINGS

The attached sheet(s) of drawings includes changes to Figues 1 and 2.

Attachment: Replacement sheet

REMARKS

In view of the above amendment, applicant believes the pending application is in condition for allowance.

In the drawings, Figures 1 and 2 have been labeled "prior art" as suggested by the Examiner.

Applicant notes the Examiner's requirement that the non-elected claims be canceled in response to a final rejection. Since the present action in non-final applicant will hold in abeyance cancellation of remaining non-elected claims until final rejection, if any, is issued.

Claims 1-19, 63-67 and 82-84 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as they invention.

Claims 1-3 and 63 are rejected under 35 U.S.C. § 102(a) as being anticipated by DOC CB of IDS of July 2003.

Claims 83 and 84 are rejected under 35 U.S.C. § 103(a) as being unpatentable over art of record.

Claims 4-19, 64-67 and 84 are allowable.

Although the Examiner states that the present invention is anticipated by Kudo's document, Applicants do not agree with the Examiner. The abstract of the Kudo's document only mentions nine security requirements and the use of three subprotocols, but their details are not described in the abstract (see last line of the abstract).

The cited Kudo document relates to a secure electronic sealed-bid auction protocol, wherein in order to satisfy the nine security requirements listed in the abstract (also in Table 2), auction is performed by bidders and a requestor using an auction service provider (auctioneer),

key service provider and time service provider. It is clearly described in the second paragraph of section 4, that "we assumed that all parties use the same public key cryptographic component", and the descriptions about "Bidding Request" at 12-16the lines of section 5.3.2 and Table 8(b) suggest that a set of the bidding value PRICE and a random value Y is encrypted as expressed by E_{KEY}(PRICE, Y) which is sent to the requester. Further, in the last paragraph headed "Auction Response" of section 5.3.3, it is described that the auction service provider decrypts E_{KEY}(PRICE, Y) and determines who won the auction.

According to the Kudo's system, the auction service provider decrypts each E_{KEY}(PRICE, Y) of all the bidders to determine the largest (or smallest) bidding value PRICE; this means that the auction service provider also knows those bidding values PRICE of other bidders in addition to the winner's bidding value PRICE.

On the other hand, according to the present invention, every participant device (participant device may correspond to a bidder in Kudo's document) has a distinct initial value and generates aimed value information by processing the initial value with a one-way function by a number of times corresponding to an aimed value (the aimed value may correspond to bidding value PRICE in the Kudo's document); each participant device or server device processes the initial value with the one-way function to generate updated initial value, and update is repeated until agreement is detected between the updated initial value and the value of the aimed value information. Thus, the principle of the invention completely differs from that of the cited Kudo's document.

According to the present invention, the server device can obtain the knowledge of maximum (or minimum) aimed value, but cannot obtain any knowledge of the other aimed values. Therefore, the system according to the present invention is higher in security than the Kudo's system.

In view of the above, consideration and allowance are, therefore, respectfully solicited.

In the event the Examiner believes an interview might serve to advance the prosecution of this application in any way, the undersigned attorney is available at the telephone number noted below.

The Director is hereby authorized to charge any fees, or credit any overpayment, associated with this communication, including any extension fees, to CBLH Deposit Account No. 22-0185, under Order No. 20162-00561-US from which the undersigned is authorized to draw.

Dated: September 16, 2008

Respectfully submitted,

Electronic signature: /Morris Liss/
Morris Liss
Registration No.: 24,510
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant